|  |  |  |
| --- | --- | --- |
| Policy #: | Title: | Effective Date: |
| x.xxx | Risk Assessment Policy | MM/DD/YY |

PURPOSE  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

To ensure that Information Technology (IT) performs risk assessments in compliance with IT security policies, standards, and procedures.

REFERENCE  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-60, NIST SP 800-70, NIST SP 800-100, NIST SP 800-115; NIST Federal Information Processing Standards (FIPS) 199

POLICY  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This policy is applicable to all departments and users of IT resources and assets.

1. SECURITY CATEGORIZATION

IT Department shall:

* 1. Apply proper security controls to data categorized as confidential by system owners, including protected health information (PHI) and personally identifiable information (PII), in accordance with applicable federal and state laws, directives, policies, regulations, standards, and guidance.
  2. Document the security controls (including supporting rationale) in the security plan for the information system.

1. RISK ASSESSMENT

IT Department shall:

* 1. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.
  2. Document risk assessment results in annual IT Risk Assessment.
  3. Review risk assessment results quarterly.
  4. Disseminate risk assessment results to stakeholders.
  5. Update the risk assessment quarterly or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

1. VULNERABILITY SCANNING

IT Department shall:

* 1. Scan for vulnerabilities in the information system and hosted applications quarterly and/or randomly in accordance with [entity defined process] and when new vulnerabilities potentially affecting the system/applications are identified and reported.
  2. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:

1. Enumerating platforms, software flaws, and improper configurations.
2. Formatting checklists and test procedures.
3. Measuring vulnerability impact.
   1. Analyze vulnerability scan reports and results from security control assessments.
   2. Remediate legitimate vulnerabilities within one month in accordance with an organizational assessment of risk.
   3. Share information obtained from the vulnerability scanning process and security control assessments with the Chief Information Officer to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
   4. Employ vulnerability scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.
   5. Update the information system vulnerabilities scanned monthly, prior to a new scan, or when new vulnerabilities are identified and reported.
   6. Ensure that information systems implement privileged access authorization to all systems for selected vulnerability scanning.

COMPLIANCE

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

RESPONSIBLE DEPARTMENT  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chief Information Office and Information System Owners

DATE ISSUED/DATE REVIEWED  
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| Date Issued: | MM/DD/YYYY |
| Date Reviewed: | MM/DD/YYYY |